

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF VIRGINIA
ROANOKE DIVISION

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
TWITTER ACCOUNTS KATIEKITTY666,
KATIE79136538, KITTY70860648, AND
NIISAYSBII THAT IS STORED AT
PREMISES CONTROLLED BY X CORP.

Case No. 6:23mj28

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Mary Echols, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with Twitter accounts KatieKitty666, Katie79136538, Kitty70860648, and Niisaysbii (hereinafter referred to as to as the “TARGET ACCOUNTS”) that are stored at premises owned, maintained, controlled, or operated by X Corp., an electronic communications service and/or remote computing service provider headquartered at 1355 Market Street, Suite 900, San Francisco, CA.

2. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. § 2703(a), (b)(1)(A) and (c)(1)(A) to require X Corp. to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

3. I am a Special Agent with the Federal Bureau of Investigation (FBI) assigned to the Richmond, Virginia, Field Office, Charlottesville Resident Agency. I have been employed with the FBI since November 2017. I investigate criminal violations relating to child exploitation, including the illegal production, transportation, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252, and 2252A; enticement of minors to engage in unlawful sexual activity, in violation of 18 U.S.C. § 2422(b); and travel with intent to engage in unlawful sexual activity, in violation of 18 U.S.C. § 2423(a). I have reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media. I also have experience in interviewing and in interrogation techniques, arrest procedures, the execution of searches, and various other criminal laws and procedures. I have personally participated in the execution of search warrants involving the search and seizure of computer equipment, electronics, cloud-storage accounts, and social media accounts. Prior to becoming a Special Agent, I was assigned to the Atlanta, Georgia, FBI Office's crimes against children unit, providing tactical and administrative assistance for child sexual exploitation investigations, which included providing support during the execution of search warrants.

4. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 2251 (production of child pornography), 2252A (distribution, receipt and possession of child pornography), and 2422 (online enticement) have been committed by the individuals identified below. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, and/or fruits of these crimes further described in Attachment B.

TECHNICAL TERMS

6. The following definitions apply to this affidavit:

7. “Computer,” as used herein, refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device” and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).

8. “Minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

9. “Sexually explicit conduct,” as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

10. “Visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

11. “Child pornography,” as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit

conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

12. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

13. A “Website” consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

14. “Discord” is a free communications app that allows its users to share voice, video, and text chat with persons on the Internet as well as browse and share any website content with those whom the user selects while still within the Discord platform. Unlike other messaging apps, Discord usernames - not phone numbers - are the basis for Discord user accounts. Discord usernames are unique, can never be replicated, and are the only publicly available identifier Discord can use to identify a Discord account to law enforcement. The company cannot identify users using phone numbers, first and last name (display name), or email address. Each unique username has a corresponding unique User ID.

PROBABLE CAUSE

15. This search warrant seeks to gather information from four Twitter accounts (the TARGET ACCOUNTS) used by a 14-year-old minor victim (hereinafter “V1”). V1 has confirmed that she used Twitter to distribute child sexual abuse material and to find individuals to whom V1 could distribute child sexual abuse material via other platforms.

16. On February 24, 2023, at approximately 10:25 PM, the FBI received a call from the Lynchburg Police Department notifying the FBI that the Lynchburg Communications Center received a report that Derrick Loi (LOI), who the caller reported to be 28 years old, had traveled from the state of New York for the purpose of engaging in sexual intercourse V1. The complainant stated that LOI was waiting to meet V1 on McVeigh Road in Lynchburg, Virginia, which is within the Western District of Virginia. LOI told V1 he would take her to a hotel to have sex. Officers from the Lynchburg Police Department responded to V1's address to make contact with her while additional officers responded to McVeigh Rd, where LOI was parked. LOI was initially identified by a photograph provided to the officers by V1 and later was fully identified as 26-year-old Derrick LOI of Lakeville, NY. Officers placed him into investigative detention.

17. After confirming LOI made a hotel reservation in the Lynchburg area, the Lynchburg police transported LOI to the Lynchburg Police Department, where an interview of LOI was conducted. During the interview, LOI confirmed he had driven from New York to Lynchburg, Virginia, to meet someone he had been speaking to online. LOI believed he was talking to someone named "Katie." LOI told the interviewing officer that his Discord usernames were "LPKensei" and "Callthevoid." LOI stated he and "Katie" discussed "hooking up," but he denied knowing how old she was. LOI stated he had requested and received photographs of a "lewd nature" from "Katie." LOI stated he and "Katie" used the Discord chat, video, and audio features. LOI stated that he met "Katie" on Twitter before moving to Discord.

18. V1's parents gave law enforcement a laptop utilized by V1 and further provided law enforcement consent to conduct a forensic examination of the laptop. An examination of the laptop gave the FBI access to V1's Discord account.

19. In reviewing V1's Discord account with the username "katieeee#5383," I observed an exchange of messages between V1 and username "callduvide#1772" dated February 14, 2023, through February 24, 2023. In the early conversation between LOI and V1, on February 14, 2023, V1 told LOI that she was fourteen years old. Throughout the conversation, LOI repeatedly requested pornographic images from V1 and discussed traveling from New York to Lynchburg, Virginia, to engage in sexual intercourse with V1.

20. On February 14, 2023, LOI stated "Ooh I can't wait to try out your kiddie holes" LOI suggested he could be her "sugar daddy" and pay her weekly. LOI provided money to V1 in exchange for child pornography. On February 14, 2023, LOI asked for a "pussy spread" photograph and V1 sent an image depicting herself bent over, using her hands to spread and expose her genitals and anus. Based on my training and experience, this photograph constitutes child pornography as that term is defined under 18 U.S.C. § 2256.

21. During the conversation, LOI discussed taking V1's virginity and discussed V1 taking birth control. LOI told V1 he was bringing vodka and sex toys when he came down to Lynchburg to meet her and sent V1 photographs of those items. LOI discussed with V1 the possibility of staying in a hotel overnight and questioned V1 about her parents' response if she did not return home. LOI instructed V1 to tell her parents she was staying with a friend the night she planned to meet him. LOI also asked V1 what she thought about age of consent laws and LOI stated "13 sounds like a good age." On February 22, 2023, LOI told V1 he was going to travel down to Virginia that weekend. LOI asked V1 if they could film their sexual encounter when he traveled down to have sex with her and continued by stating "...hopefully I get good footage."

22. On February 24, 2023, LOI instructed V1 to "take a pic of ur pussy rn." V1 responded by sending an image depicting herself nude, exposing her genitals. Based on my training

and experience, this photograph constitutes child pornography as that term is defined under 18 U.S.C. § 2256.

23. On May 25, 2023, LOI was indicted by a federal grand jury in the Western District of Virginia in a four-count indictment charging him with one violation of 18 U.S.C. § 2422(b), one violation of 18 U.S.C. § 2423(b), one violation of 18 U.S.C. § 2251, and one violation of 18 U.S.C. § 2252A(a)(5)(B).

24. While reviewing the laptop utilized by V1, your affiant observed an exchange of messages between another Discord account known to be used by V1 and a Discord account with the username “Jeffthepumpkin#2260,” dated January 2, 2023, through January 30, 2023.

25. On January 3, 2023, the user of the Jeffthepumpkin#2260 Discord account sent to V1 a picture that he identified as himself. Law enforcement located a social media account in the name of “Andrew Kent,” and the social media profile picture was identical to the picture sent by the user of the Jeffthepumpkin#2260 Discord account. Based on this and other information, the user of this Discord account was determined to be Andrew Kent (KENT).

26. Early in the Discord conversation between KENT and V1, on January 3, 2023, KENT asked V1 her age and V1 responded that she was fourteen years old. Throughout the conversation, KENT repeatedly requested pornographic images from V1. On January 3, 2023, KENT told V1 “I want to take a kid’s virginity.”

27. On January 17, 2023, KENT asked V1 for photos depicting her “pussy.” V1 responded by sending an image depicting herself nude, exposing her genitals. KENT asked for another photo depicting her “last hole,” and V1 sent an image depicting herself nude, exposing her anus. Based on my training and experience, these photographs constitute child pornography as that term is defined under 18 U.S.C. § 2256.

28. On January 23, 2023, KENT told V1 “Show me your kiddo parts fucktoy,” and V1 sent four images depicting her legs spread apart exposing her genitals. Based on my training and experience, these photographs constitute child pornography as that term is defined under 18 U.S.C. § 2256.

29. On January 28, 2023, KENT directed V1 “when you wake up, I want to see a picture of you on your knees spreading your holes.” V1 sent an image depicting V1 in the manner that KENT had requested. Based on my training and experience, this photograph constitutes child pornography as that term is defined under 18 U.S.C. § 2256.

30. On May 25, 2023, KENT was indicted by a federal grand jury in the Western District of Virginia in a four-count indictment charging him with one violation of 18 U.S.C. § 2422(b) and three violations of 18 U.S.C. § 2251.

31. On June 16, 2023, KENT was arrested in Kansas City, Kansas. by the FBI. In an interview with KENT, he disclosed to the agents that he used Twitter to meet minor females. He used the female persona “Tris” to meet minor females and to find out where they lived. KENT used the female persona to introduce the minor females to his social media accounts. KENT communicated with numerous minor females to include V1.

32. KENT also admitted to being the user of the “Jeffthepumpkin#2260” Discord account and to communicating with a girl from Virginia who he believed to be 14 or 15 years old. He admitted to communicating with this girl (who is believed to be V1) using Discord and Twitter. He also admitted that he first met this girl on Twitter.

33. While reviewing V1’s laptop, I observed that there were two Twitter accounts logged into the web browser of the laptop, accounts with the usernames Katie79136538 and Kitty70860648. However, I could not access the content of those accounts because they had been

suspended by Twitter. I also observed the existence of a Twitter account through screen captures saved to the laptop. The account observed in the screen captures, Niisaysbii, communicated with various other users, including a Twitter account associated with KENT. The account Niisaysbii was no longer logged into the laptop.

34. On April 10, 2023, I served an administrative subpoena on Twitter for Twitter accounts associated with an email address connected to V1's Discord account and with the Twitter handle Katie79136538. Twitter informed me that that email address was associated with another Twitter account, which had the username KatieKitty666. Twitter also informed me that it had suspended the KatieKitty666 and Katie79136538 accounts due to suspected child pornography. Subsequently, Twitter preserved the accounts. Your affiant contacted NCMEC who confirmed that KatieKitty666, Katie79136538, and Niisaysbii had been reported to NCMEC and that cyber reports had been generated.

35. FBI investigators arranged for a specially trained Child and Adolescent Forensic Interviewer (CAFI) to conduct a forensic interview of V1, which occurred on March 28, 2023. V1's memory of events as told to the CAFI corroborated the chat messages and photographs that I reviewed in her Discord account. When shown the Discord messages during the CAFI interview, V1 confirmed that these messages were exchanged between herself and LOI. VI further identified herself in the images of child pornography that she sent to LOI. V1's memory of her conversations with KENT as told to the CAFI corroborated the examination of the chat messages and photographs between V1's Discord account and KENT. When shown these messages during the CAFI interview, V1 confirmed the exchange of messages over Discord between herself and KENT. VI further identified herself in images of child pornography sent to KENT in the messages. V1 also disclosed that she met adult males online through various Twitter accounts and that the

conversation would then move over to Discord. V1 created additional Twitter accounts because her accounts kept getting suspended by Twitter.

BACKGROUND CONCERNING TWITTER¹

36. X Corp. owns and operates Twitter, a social networking and microblogging service that can be accessed at <http://www.twitter.com> and via the Twitter mobile application (“app”). Generally, Twitter allows users to register and create an account; to personalize (if desired) an account profile page; and to send and receive communications via the platform. These functionalities are discussed in more detail below.

37. Twitter permits its users to communicate via messages that can contain photos, videos, links, and/or a maximum of 280 characters of text. Users can choose to share these messages, called “Tweets,” with the public or, alternatively, to “protect” their Tweets by making them viewable by only a preapproved list of “followers.” Each Tweet includes a timestamp that displays when the Tweet was posted to Twitter. Users can also Tweet a copy of other Tweets (“retweet”) or Tweet a reply to another Tweet. Users can also indicate that they like a Tweet by clicking on a heart icon that appears next to each Tweet on the platform.

38. Twitter also permits its users to exchange private messages, known as “direct messages” or “DMs,” with other Twitter users. DMs, which also may include photos, videos, links, and/or text, can only be viewed by the sender and designated recipient(s). Direct messages may be sent to an individual user or to a group of up to 50 Twitter users. Twitter users have the ability to choose whether they can receive a direct message from anyone. At any time, a Twitter

¹ The information in this section is based on information published by Twitter on its website, including, but not limited to, the following document and webpages: “Guidelines for law enforcement,” available at <https://help.twitter.com/en/rules-and-policies/twitter-law-enforcement-support>, “Using Twitter,” available at <https://help.twitter.com/en/using-twitter>, and “New user FAQ,” available at <https://help.twitter.com/en/new-user-faq>.

user has the ability to alter the settings on their Twitter account so that they can receive direct messages only from (1) individuals to whom the user has already sent a direct message and (2) Twitter accounts that the user “follows” via his account.

39. While individuals are not required to register with Twitter to view the content of unprotected Tweets, individuals must register for a Twitter account to send Tweets, to “follow” accounts in order to view protected Tweets, and to send and receive direct messages. A user may register for an account for free by visiting Twitter’s website or via the Twitter app. When a user creates a new Twitter account, Twitter assigns that account a unique user ID (“UID”). A user must also select a password as well as a unique Twitter username (also known as a “handle”). Twitter then appends the @ symbol in front of whatever username the user selects to create the Twitter username (for example: @example). The user may also select a different name (the “display name”), which is not automatically preceded by the @ symbol, to be displayed on his profile picture and at the top of his Tweets alongside his Twitter username. The display name can include symbols similar to emojis. The user can change their password, username, and/or display name at any time, but the UID for the account will remain constant.

40. While anyone can sign up and use Twitter for free, as of November 2021 Twitter also offered a subscription model that offered users access to additional features and app customizations. This new subscription is called Twitter Blue. A user can sign up for Twitter Blue at any time. Twitter Blue allows a user to make changes to published tweets, allows users to turn on an “Undo Tweet” feature which keeps a tweet private during a set Tweet Undo period of between 5 and 60 seconds, or until the user taps “Send now,” and allows users to Tweet up to 4,000 characters.

41. At the time of Twitter account creation, X Corp. asks the user for certain identity and contact information, including: (1) name; (2) email address and/or telephone number; and (3) month and year of birth. X Corp. also keeps certain information relating to the creation of each Twitter account, including: (1) the date and time at which the user's account was created; and (2) the method of account creation (e.g., website or Twitter app).

42. Upon the creation of a Twitter account, a generic profile page is automatically created for the user. This page displays information including (1) the user's Twitter username; (2) the display name; (3) the number of Twitter accounts the user is following; (4) the number of Twitter accounts that are following the user; and (5) Tweets sent by the user (although, as noted above, if the user has chosen to protect their Tweets they will be visible only to preapproved "followers"). The user can personalize this page by posting a personal picture or image (known as an "avatar") to appear on the page and/or a banner image to appear across the top of the profile page. The user can also add text to create a short biography, to identify his location, to provide a link to his website, or to specify his date of birth.

43. As noted above, Twitter users can use their account to send and receive communications. If a Tweet includes a Twitter username that is preceded by the @ symbol, that is referred to as a "mention." The Twitter user mentioned in the Tweet will receive a notification informing them that they have been mentioned and showing the content of that Tweet. Similarly, if another Twitter user replies to a Tweet sent by a user, the user who sent the original Tweet will receive a notification that someone replied to their message, and the notification will show the content of that reply.

44. Twitter users can also include links to webpages in their Tweets and Direct Messages. Twitter automatically processes and shortens links provided by the user to a shortened link that starts <http://t.co/>. Twitter tracks how many times these shortened links are clicked.

45. A registered Twitter user can also “like” a Tweet by clicking a heart icon on a Tweet sent by another user. If another user “likes” a Tweet that is posted by the Twitter user, a notification will appear in the user’s account identifying what Tweet was liked and who liked it.

46. As noted above, users can include photographs, images, and videos in their Tweets. Each account has a “media timeline” on their profile that displays “the photos, videos, and GIF’s [the accountholder] has uploaded with [their] Tweets.” An individual can view a Twitter user’s media timeline by visiting the user’s Twitter profile page.

47. Twitter users can also opt to Tweet with their location attached. This functionality is turned off by default, so Twitter users must opt in to utilize it. However, if a Twitter user enables Twitter to access their precise location information, the Twitter user will have the option of attaching their location (e.g., the name of a city or neighborhood) to a Tweet at the time it is sent. If the user uses Twitter’s in-app camera to attach a photo or video to the Tweet while the functionality is enabled, the Tweet will include both the location label (e.g., the name of a city or neighborhood) of the user’s choice as well as the device’s precise location in the form of latitude-longitude coordinates. The user can turn this functionality off (thereby removing their location from their Tweets) at any time, and they can delete their past location data from Tweets that have already been sent.

48. A Twitter user may choose to “follow” another Twitter user. If a Twitter account is unprotected (i.e., privacy settings have not been enabled), the user can follow another user simply by clicking the “follow” button on the other user’s Twitter profile page. If a Twitter account is

protected (i.e., privacy settings have been enabled), the user can follow another user by clicking the “follow” button and waiting for the other user to approve their request. Once an account is followed by a Twitter user, the Tweets posted by the account the user follows will appear in the user’s Twitter Home timeline. Every time a Twitter user follows another account, Twitter sends a notification to the account being followed to inform them about the new follower. Each user’s Twitter profile page includes a list of the people who are following that user and a list of people whom that user follows. Twitter users can “unfollow” other users whom they previously followed at any time. Twitter also provides users with a list of “Who to Follow,” which includes a few recommendations of Twitter accounts that the user may find interesting based on the types of accounts that the user is already following and who those people follow.

49. A Twitter user can also “block” other Twitter users. This prevents the blocked account from contacting or following the user or from seeing the user’s Tweets. Twitter does not notify the user of a blocked account when another Twitter account blocks them.

50. A Twitter user can also use Twitter’s integrated search function. When a user types a search term into Twitter’s search tool, it will return results that include accounts, Tweets, and photos that match that search term. Twitter users using the service via the Twitter mobile app also have the option of saving searches that they have performed. A user can delete such saved searches at any time.

51. A Twitter user can also join or create “Lists” of other Twitter accounts. These Lists often organize Twitter accounts by group, topic, or interest. Viewing a timeline of a specific List will show you a stream of Tweets made only by accounts that are on that List. Users can pin their favorite lists to their Twitter Home timeline page. Twitter users have the ability to remove their accounts from Lists upon which it may appear.

52. Twitter also offers a functionality called “Spaces,” which it calls “a new way to have audio conversations on Twitter.” Any user can create a Space; that user is referred to as the “host.” Spaces are public, so anyone can join and listen to the conversation within a Space once it is created, although a user can send another Twitter user a link to their Space and invite them to join. By default, the only individuals permitted to speak in a Space are the individuals that the host invites to do so, although this setting can be modified to allow a broader set of individuals to speak. Up to 13 people can speak in a Space at a given time.

53. Twitter also offers the ability to sign into third-party apps and websites using one’s Twitter account. Typically, the third-party app or website will have a link that enables the user to sign into the third-party service using their Twitter account. Doing so grants the third-party service access to the Twitter user’s account. Depending on the authorizations the Twitter user gives to the third-party service, the third-party service may be able to read the user’s Tweets, see who the user follows on Twitter, post Tweets to the user’s profile, or access the user’s email address. A user can revoke a third-party app or website’s authorization to access their Twitter account and associated data at any time.

54. X Corp. collects and retains information about a user’s use of the Twitter service, to include: (1) content of and metadata relating to Tweets and Direct Messages; (2) photos, images, and videos that are shared via Twitter and stored in the user’s Media Timeline; (3) the identity of the accounts that a user follows and the accounts that follow the user’s account; (4) the content uploaded to a user’s profile page, including their avatar, banner image, and bio; (5) information about Tweets the account has liked; (6) information about Lists associated with the account; (7) information about the Spaces that a user has participated in, including the host of the Space, its start and end times, and information about other attendees; and (8) applications that are connected

to the Twitter account. X Corp. also collects and retains various other data about a user and his/her activity, including:

- a. logs of Internet Protocol (“IP”) addresses used to log in to Twitter and the timestamp associated with such logins;
- b. transactional records reflecting, for example, when a user changed their display name or email address;
- c. the identities of accounts that are blocked or muted by the user; and
- d. information relating to mobile devices and/or web browsers used to access the account, including a Twitter-generated identifier called a UUID that is unique to a given device.

55. In some cases, Twitter users may communicate directly with X Corp. about issues relating to their account, such as technical problems or complaints. Social networking providers like X Corp. typically retain records about such communications, including records of contacts between the user and the provider’s support services, as well as records of any actions taken by the provider or user as a result of the communications. X Corp. may also suspend a particular user for breaching X. Corp.’s terms of service, during which time the Twitter user will be prevented from using Twitter’s services.

56. Additionally, providers of electronic communications services and remote computing services often collect and retain user-agent information from their users. A user agent string identifies, among other things, the browser being used, its version number, and details about the computer system used, such as operating system and version. Using this information, the web server can provide content that is tailored to the computer user's browser and operating system.

57. In my training and experience, evidence of who was using a Twitter account and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

58. Based on my training and experience, direct messages, photos, and videos are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. Thus, stored communications and files connected to a Twitter account may provide direct evidence of the offenses under investigation and can also lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

59. In addition, the user’s account activity, logs, stored electronic communications, and other data retained by X Corp. can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, subscriber information, messaging logs, photos and videos (and the data associated with the foregoing, such as geolocation, date and time) may be evidence of who used or controlled the account at a relevant time. Similarly, device identifiers and IP addresses can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

60. Account activity may also provide relevant insight into the account owner’s state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner’s motive and intent to commit a crime (*e.g.*, information indicating a plan

to commit a crime), or consciousness of guilt (*e.g.*, deleting account information in an effort to conceal evidence from law enforcement).

61. Other information connected to the use of an account may lead to the discovery of additional evidence. For example, accounts are often assigned or associated with additional identifiers such as account numbers, advertising IDs, cookies, and third-party platform subscriber identities. This information may help establish attribution, identify and link criminal activity across platforms, and reveal additional sources of evidence

62. Therefore, X Corp.'s servers are likely to contain stored electronic communications and information concerning subscribers and their use of Twitter. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

CONCLUSION

63. Based on the forgoing, I request that the Court issue the proposed search warrant.

64. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on X Corp. Because the warrant will be served on X Corp., who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,



MARY ECHOLS
SPECIAL AGENT
FBI

Received by reliable electronic means and sworn and attested to by telephone on this 20th day of July 2023.

Robert S. Ballou

HONORABLE ROBERT S. BALLOU
UNITED STATES DISTRICT JUDGE